

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Modernizing the E-Rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	
	)	

**COMMENTS OF COX COMMUNICATIONS, INC.**

**I. Introduction**

Cox Communications, Inc., (“Cox”) hereby submits these comments in support of the Federal Communications Commission’s (“Commission”) proposal to make permanent funding for internal connections and supporting services under the E-Rate program and urging the Commission to expand the scope of services eligible for E-Rate funding.<sup>1</sup> In 2014, the Commission adopted the “category two” budget approach, which set five year budgets for schools and libraries that provide a set amount of funding to support internal connections, connections needed for broadband connectivity within schools and libraries.<sup>2</sup> This approach, however, is scheduled to sunset in funding year 2020.<sup>3</sup> The Commission also provided funding for managed internal broadband services, caching and basic maintenance for internal connections until funding year 2019.<sup>4</sup> We agree with the Commission that continued permanent E-Rate support for internal connections and managed internal broadband services, caching and basic maintenance for internal broadband services is necessary to ensure that the program continues to meet the needs of today’s schools and libraries, because these services enable one-to-one digital learning and other computer-based curriculum through a variety of devices. We also believe that the continuing evolution of technology to the cloud and escalating cybersecurity issues warrant a fresh look at additional service eligibility.

---

<sup>1</sup> *Modernizing the E-Rate Program for Schools and Libraries*, Notice of Proposed Rulemaking, FCC 19-58, para. 14 (rel. July 9, 2019) (“*NPRM*”).

<sup>2</sup> *Modernizing the E-Rate Program for Schools and Libraries*, Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, 8898-922 (2014) (“*2014 First E-Rate Order*”).

<sup>3</sup> 47 CFR § 54.502(b).

<sup>4</sup> *2014 First E-Rate Order*, paras 123-130, 29 FCC Rcd at 8918-8921.

## **II. Category Two Budget Approach for Internal Connections and Supporting Services Should be Made Permanent**

Cox fully supports the Commission's proposal to extend permanently the category two budget approach for internal connection support.<sup>5</sup> Cox agrees with the Commission that the category two budget approach has been generally successful in ensuring that category two support is widely disbursed in all fifty states and territories and to applicants at all discount levels.<sup>6</sup> The Commission should ultimately adopt a budget approach which continues to distribute fairly support among schools and libraries, but regardless of any changes made, the Commission must provide certainty to schools and libraries that category two funding for internal connections will continue permanently to ensure that program rules do not distort purchasing decisions. If schools and libraries believe that the Commission may rescind support for internal connections or are otherwise uncertain if funding will continue after a set period of time, it may incent schools and libraries to, for example, buy Wi-Fi equipment, rather than consider leased managed Wi-Fi services, even if they would otherwise prefer the benefits and effectiveness of a managed solution, to take advantage of "soon-to-disappear" funds.

The Commission also sought comment on extending the eligibility of managed internal broadband services, caching and basic maintenance of internal connections beyond funding year 2019.<sup>7</sup> Cox is strongly in favor of making support for managed internal broadband services, caching and basic maintenance of internal connections permanent under whatever permanent category 2 budget approach is adopted. These managed internal broadband services can provide substantial benefits and cost savings to many schools and libraries, particularly small districts and libraries without dedicated technology staff available to deploy and manage advanced LANs/WLANs quickly and efficiently. Providing this support during the time-limited period established by the Commission has not resulted in exorbitant requests or demand and not created any undue hardship from an administrative perspective, so there is no reason to withhold these viable solutions from E-Rate participants. However, as stated above, it is important that the Commission make funding permanent to avoid unintended purchasing incentives, such as

---

<sup>5</sup> *NPRM* at para. 14.

<sup>6</sup> *NPRM* at para. 15.

<sup>7</sup> *NPRM* at para. 18.

applicants choosing to purchase WiFi equipment rather than leased managed WiFi services because of uncertainty that funding will continue after a set time period.

### **III. All Virtualized Solutions Should be Eligible for Support**

In addition to issues related specifically to the category two budget approach, the Commission sought comment more broadly on any other category two eligibility issues that should be considered.<sup>8</sup> Although the Commission has explicitly stated that hardware and software solutions that virtualize the functionalities of eligible internal connections equipment are eligible for E-Rate support, it has emphasized that *only* virtualized solutions that perform the functions of eligible broadband internal connections are eligible.<sup>9</sup> As cloud infrastructure and enhanced connectivity platforms such as SD-WAN have become more available in addition to cloud-based versions of internal connections since 2014, the lines between internal connections and connections to the Internet have blurred, with virtualized, cloud-based technologies being able to provide both types of functionality. The Commission should no longer restrict support to virtualized eligible internal connections, rather it should support virtualized equivalents of eligible category one and category two equipment and services. Provided the function that the virtualized solution performs is eligible, the fact that it is associated with a cloud-based solution, not a hardware-based solution, should be irrelevant. Virtualized solutions may be preferred or more cost-effective than their hardware-based equivalents, when taking into account equipment maintenance, down time and equipment obsolescence. Schools and libraries should not be precluded from considering virtualized options, just because the technology is new or virtual. Moreover, so long as schools and libraries are required to consider cost as a primary factor and allocate costs between eligible and ineligible functions, support for virtualized solutions for category one and category two equipment and services should not overly burden the E-Rate program. If demand for virtualized solutions becomes unreasonably high, the Commission can always adopt measures to prioritize or cap requests for such services, or as it has before, track spending trends and revisit if new demand reaches a certain percentage of overall E-Rate support.

---

<sup>8</sup> *NPRM* at para. 18

<sup>9</sup> 2014 *First E-Rate Order*, para. 119, 29 FCC Rcd at 8917. See also *Modernizing the E-rate Program for Schools and Libraries*, Order, para. 19, 30 FCC Rcd 9923, 9929-9930 (WCB 2015).



#### IV. Network Security Services to Prevent and Recover from Cyber Attacks Should be Eligible for Category Two Support

Finally, the Commission sought comment on additional services that should be made eligible under category two funding.<sup>10</sup> The time has come for the Commission to revisit its 2014 decision to exclude “further network security services,” such as DDoS attack prevention and mitigation services.<sup>11</sup> The challenges facing school and library system information technology (“IT”) departments across the country have grown aggressively since 2014, while IT budgets have faced increasing pressure.<sup>12</sup> At the same time IT budgets are squeezed in the education space, the complexity of technology, the diversity of skills needed to support it and the threats to networks, sensitive data and operations systems are expanding at an exponential rate. For example, school and library systems have experienced a marked increase in the number of DDoS and ransomware attacks,<sup>13</sup> at a time when few if any school systems possess the technical or financial resources to effectively combat them. As such, an effective means of addressing this exposure is to enlist the assistance of companies that can provide the software, equipment, services and personnel to secure the school system’s IT operations and possibly provide those things in an as-a-service, operating

---

<sup>10</sup> *NPRM* at para. 18.

<sup>11</sup> See *2014 First E-Rate Order*, para 121 & n. 275, 29 FCC Rcd at 8918 (declining to designate services suggested by commenters, including intrusion protection and detection, malware protection, application control, content filters, DDoS mitigation, and cybersecurity services, as eligible in three sentences).

<sup>12</sup> Most public school systems have seen operating budgets grow at a rate that barely overcomes inflation and have seen a reduction in payrolls that would support internal IT operational capacity. According to the National Center for Educational Statistics (NCES), since the year 2000, the percentage of budget allocated to payroll has fallen 7% (from 64% to 57%) while both employee benefits and purchased services has risen over the same period. See [https://nces.ed.gov/programs/coe/indicator\\_cmb.asp](https://nces.ed.gov/programs/coe/indicator_cmb.asp).

<sup>13</sup> See, e.g., “Louisiana Governor declares emergency after ransomware attack hits three schools,” <https://cyware.com/news/louisiana-governor-declares-emergency-after-ransomware-attack-hits-three-schools-50569756>; “New Haven Public Schools hit with ransomware attack,” <https://cyware.com/news/new-haven-public-schools-hit-with-ransomware-attack-7079b9a7>; “Syracuse Schools, Libraries Disabled by Ransomware Attack,” [https://www.govtech.com/education/Syracuse-Schools-Libraries-Disabled-by-Ransomware-Attack.html?utm\\_term=READ%20MORE&utm\\_campaign=New%20York%20School%20District%20Changes%20Facial%20Recognition%20Policy&utm\\_content=email&utm\\_source=Act-On+Software&utm\\_medium=email](https://www.govtech.com/education/Syracuse-Schools-Libraries-Disabled-by-Ransomware-Attack.html?utm_term=READ%20MORE&utm_campaign=New%20York%20School%20District%20Changes%20Facial%20Recognition%20Policy&utm_content=email&utm_source=Act-On+Software&utm_medium=email); “Connecticut School District Hit with Ransomware Attack,” <https://www.govtech.com/security/Connecticut-School-District-Hit-with-Ransomware-Attack.html>; “Ransomware attack on Oklahoma City Public Schools,” <https://www.cybersecurity-insiders.com/ransomware-attack-on-oklahoma-city-public-schools/>; “Coventry Public Schools’ computers attacked with malware,” [https://turnto10.com/i-team/nbc-10-i-team-coventry-public-schools-computers-attacked-with-malware?fbclid=IwAR3s6UePp-OB5ZqdM2lGsp\\_Mevi7s31uOt5HGg0PKa2BO4kx27ZKDI3VWU](https://turnto10.com/i-team/nbc-10-i-team-coventry-public-schools-computers-attacked-with-malware?fbclid=IwAR3s6UePp-OB5ZqdM2lGsp_Mevi7s31uOt5HGg0PKa2BO4kx27ZKDI3VWU), “Back to School DDoS Attacks Blocks Parents and Students Across the U.S.,” <https://www.secureworldexpo.com/industry-news/ddos-attack-example>; “DDoS-for-Hire Services Doubled in Q1,” <https://www.darkreading.com/perimeter/ddos-for-hire-services-doubled-in-q1-/d/d-id/1335042>.

expense format. Unfortunately, without the support of E-Rate, the funds for such services aren't in the typical school system's budget.

A DDoS attack is an attempt from an outside individual or group to overload network systems, equipment and memory resources. DDoS attacks are unique from other types of malware or viruses, because they do not simply slow down Internet service; they can cripple systems and effectively result in a temporary loss of Internet service. In addition, certain types of reflective DDoS attacks<sup>14</sup> can saturate Internet broadband circuits, leaving local firewall appliances helpless to restrict unwanted traffic. Ransomware is a type of malware that locks a target's files, data or the PC itself and extorts money in order to provide access. Available DDoS and Ransomware services include monitoring school and library networks for DDoS attacks and malware and mitigation of attacks by filtering out unwanted traffic. Products and services that mitigate malware, including ransomware, would include, for example, a next generation firewall, which includes intrusion detection, AV Malware protection, and content filtering; end point protection, such as AV malware software installed on a PC or MAC; and a recursive DNS firewall.

Because DDoS and ransomware attacks can render Internet service effectively unusable, support for DDoS and Ransomware prevention and restoration services and equipment is necessary to protect the E-Rate fund's investment in Internet access, internal connections, and the integrity of educational networks. The Commission's first goal in modernizing the E-Rate program was "ensuring affordable access to high-speed broadband sufficient to support digital learning in schools and robust connectivity for all libraries."<sup>15</sup> Inclusion of DDoS and Ransomware attack prevention and mitigation equipment and services will further this goal by ensuring that schools and libraries have the protection necessary for continued access to the high-speed services made possible by the E-Rate program.<sup>16</sup> The Commission should also clarify that E-Rate should provide support for equipment and services, including virtualized services, which perform eligible functions, in this case, cybersecurity asset protection and restoration functions.

---

<sup>14</sup> A reflective attack may involve sending forged requests to a large number of computers that will reply to the requests and send those replies to the targeted victim through the use of Internet Protocol address spoofing.

<sup>15</sup> *2014 First E-Rate Order*, 29 FCC Rcd at 8881, para. 26.

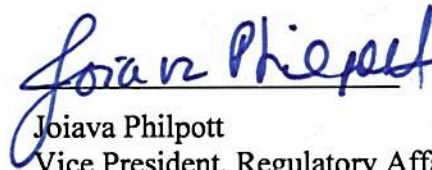
<sup>16</sup> Network security services that protect against and help systems recover from DDoS and Ransomware attacks protect assets used to provide internal connections and could be considered category two expenses. However, they also protect assets used to provide Internet access, so they could alternatively be funded under category one. In either case, support would protect assets purchased with E-Rate funds.

## V. Conclusion

Based on the reasons outlined herein, Cox respectfully requests that the Commission make permanent funding for the category two budget approach for internal connections, managed internal broadband services, caching, and basic maintenance of internal connections; clarify that virtualized equivalents of both Category One and Category Two eligible equipment, services, and functionalities are eligible for support; and expand the Category Two eligible services list to include cyber security equipment and services which prevent and respond to DDoS and Ransomware attacks.

Respectfully submitted.

By:



Joiava Philpott  
Vice President, Regulatory Affairs  
Cox Communications, Inc.  
6205 Peachtree Dunwoody Road  
Atlanta, GA 30328

Barry J. Ohlson  
Jennifer L. Prime  
Cox Enterprises, Inc.  
975 F Street, NW, Suite 300  
Washington, DC 20004  
202-637-1330

August 16, 2019